(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/35348 A1

(51) International Patent Classification[7]: G07C 9/00, G06F 17/60

(21) International Application Number: PCT/US00/27261

(22) International Filing Date: 4 October 2000 (04.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/437,103 9 November 1999 (09.11.1999) US

(71) Applicant: IRISCAN, INC. [US/US]; Suite E, 9 East Stow Road, Marlton, NJ 08053-3159 (US).

(72) Inventors: MUSGRAVE, Clyde; 3620 Fairfield Pl., Frisco, TX 75035 (US). CAMBIER, James, L.; 10 Holly Drive, Medford, NJ 08055 (US).

(74) Agents: DONOHUE, John, P., Jr. et al.; Woodcock Washburn Kurtz Mackiewicz & Norris LLP, 46th floor, One Liberty Place, Philadelphia, PA 19103 (US).

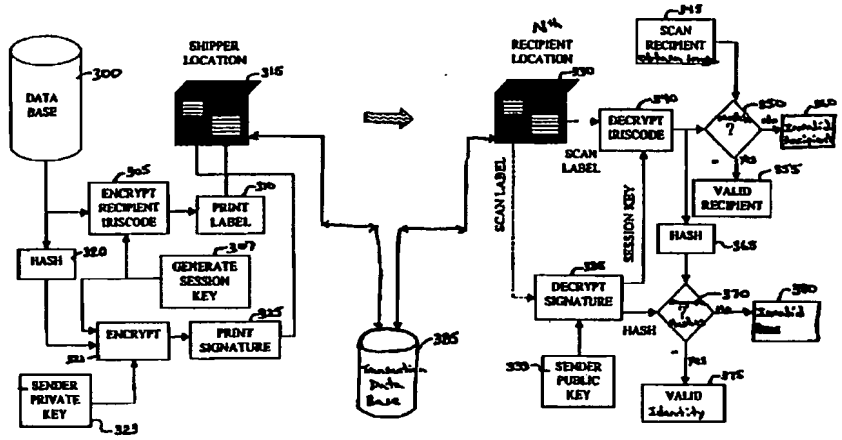
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATION OF SHIPPING TRANSACTIONS USING PRINTABLE AND READABLE BIOMETRIC DATA



(57) Abstract: A system and method that use iris recognition to ensure secure shipping transactions is provided. A system and method for printing unique biometric identification codes, particularly those derived from the iris of the eye, to goods or documents being shipped from one point or individual to another. The sender's iris is captured when the package is picked up and the resulting biometric template is included in a printable and readable biometric data printed on a label and attached to the package. The shipper compares the printed template with a stored template from a database of previously enrolled customers to authenticate the identity of the sender. The biometric template of the intended recipient can be retrieved from the same database and attached to the package so it may be compared to the template generated by capturing an image of the iris of the recipient upon delivery. Methods for encrypting the codes to prevent tampering and reading the printed printable and readable biometric data using standard scanning equipment are also described.

WO 01/35348 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR AUTHENTICATION OF SHIPPING TRANSACTIONS USING PRINTABLE AND READABLE BIOMETRIC DATA

FIELD OF THE INVENTION

The present invention relates in general to biometric authentication of physical characteristics of a human being. More particularly, the present invention relates to using iris recognition to authenticate the identity of one or more persons involved in a shipping transaction thereby ensuring a secure shipping transaction.

BACKGROUND OF THE INVENTION

In the shipping of high-value materials and documents there is often a requirement to uniquely and reliably identify one or more of a sender and a receiver. In addition, it is also sometimes desirable to authenticate the identity of shippers, or carriers, involved in the shipping transaction. For example, a significant problem in the shipping industry is the theft of high-value packages from within storage or transport facilities operated by a shipping company. Often a high-value package is identified as such by the names and/or addresses of the sender and/or the receiver. A person may recognize a package as possibly containing high-value goods because of knowledge of the type of business of the sender and/or the receiver, or the lifestyle of the sender and/or the receiver.

Currently the recipient's signature is often, but not always, recorded by the shipping company representative at the time the package is delivered in an attempt to ensure the secure delivery of the package. Typically, "high-value" packages require a positive

acknowledgment by signatures and a clear transfer of liability from a shipper to a receiver. However the signature may be illegible and in any case is subject to forgery. Hence, this conventional system and method provide insufficient protection, especially against liability claims, particularly when the value of the goods is very high.

High value packages are typically stored in specially constructed and restricted areas having limited access via, for example, badging. The identification of employees of the shipping agent who are responsible for the security of the special areas is another key element of liability protection for the shipper/carrier.

Other technologies exist for ensuring the security of goods being shipped between multiple points. These technologies include, for example, bar codes. Packages labeled with machine-readable bar codes give them a unique identity (e.g., "tracking number") to facilitate timely and accurate delivery. However, one-dimensional bar codes require an access code that serves as a real-time key for opening a database. This has the disadvantage of requiring an external database after the bar code has been scanned. In addition, these existing codes provide no assurance of the authenticity of sender or receiver.

Biometrics, such as fingerprints, have come into widespread use for personal identification, but there exists no single standard analysis technique or code format. Due to the lack of a single standard and the poor accuracy, other biometrics are of very little value in this type of application.

Moreover, traditional security techniques only ensure that token of identity are checked, but do not obscure the nature of the goods or the identity of the shipper or receiver. They simply check the token and do not provide a means of authenticating the identity of the sender or receiver. Therefore, they are subject to fraudulent use associated with the sender, the receiver, or other persons involved in the shipping process. The fraud can include, for example, theft, substitution of inferior goods, alteration of the goods, or mishandling of the goods.

In addition to the shipping transaction security technologies discussed above, various technologies are used for verifying the presence of a person in accordance with an examination of particular biometric attribute of the person, such as the attributes of voice recognition, face recognition, fingerprints, hand geometry, and retinal scanning. Unlike DNA and iris recognition, which are true identifiers, these other biometrics do not verify the identity

of a person. The latter of these technologies, retinal scanning involves the visual examination of the particular attributes of the exterior of the iris of at least one of the person's eyes. The iris of the human eye has random patterns of striations, ciliary processes, crypts, rings, furrows and other features which had been shown capable of generating highly unique biometric templates for personal identification. In this regard, reference is made to U.S. Patent No. 4,641,349, "Iris Recognition System", issued to Flom et al., and U.S. Patent No. 5,291,560, "Biometric Personal Identification System Based on Iris Analysis", issued to Daugman. As made clear by these patents, the visible texture of a person's iris can be used to distinguish one person from another with great accuracy. Thus, iris recognition can be used for such purposes as identifying a person in various applications, such as controlling access to a secure facility or a bank automatic teller machine, for example. An iris recognition system involves the use of an imager to video image the iris of each person attempting access, and image processing means for comparing this iris video image with a reference iris image on file in a database.

What is still needed is a system and method which solve the aforementioned problems associated with ensuring secure shipping transactions. As will be seen, the present invention provides an improved system and method for ensuring secure shipping transactions which solve the aforementioned problems.

SUMMARY OF THE INVENTION

The present invention is directed to a system that uses iris recognition to authenticate the identity of a person in a shipping transaction involving the movement of goods between multiple points, or destinations. The system of the present invention includes a sender, a receiver, one or more shippers, one or more biometric imaging devices, one or more processors, a printer, a reader, and a label having printable and readable biometric data, hereinafter also referred to as IriStrip™ data. Preferably, the IriStrip™ data is a 2-D bar code and the indicia of the bar code include at least one iris template of one or more person in the shipping transaction, such as the sender, the receiver, or a shipper. The IriStrip™ data can also include other shipping information, such as information about the goods, shipping instructions, handling instructions, the point of orientation, the point of destination, etc. Preferably, the IriStrip™ data is encrypted using authorized encryption techniques before it is printed on the label. The label is printed and attached to the goods and the reader is used

by persons involved in the shipping transaction to read the IriStrip™ data at each destination in the shipping transaction to track the movement of the goods and to authenticate the identity of one or more person involved in the shipping transaction. Attached to the goods, the biometric template of the IriStrip™ data allows later detection of fraud associated with the shipping transaction, including theft, substitution of inferior goods, alteration of the goods, mishandling of the goods, etc.

The present invention is also directed to a method of providing secure shipping of goods between two points using iris recognition techniques to authenticate the identity of one or more person in the shipping transaction. The method comprises obtaining an image of an iris of at least one eye of a designated receiver of the goods and printing a label having printable and readable biometric data, or IriStrip™ data. Preferably, the method includes encrypting the printable and readable data in the indicia of a 2-D bar code and includes one or more biometric templates (e.g., an IrisCodes™ template). The printable and readable data can include other identification and shipping information, such as, for example, the name, address, and phone number of the sender and/or receiver, the type, quantity, and condition of the goods, insurance information, shipping instructions, handling instructions, etc. The method further includes, attaching the label to a package, document, or goods to be shipped, shipping the package between a point of origination and a point of destination, obtaining an image of an iris of at least one eye of a receiver of the goods, comparing one of the obtained iris images to iris images stored in the printable and readable data, or alternatively a database, and authenticating the security of the shipping transaction based on the comparison.

The present invention can also provide for the authentication of the identity of the sender of the package. Once the package has been successfully delivered to the designated recipient, a return label having a printable and readable data containing identification data relating to the sender can be read, or scanned, to obtain a digital signature contained therein. If the digital signature has been encrypted (e.g., digitally sign, compute hash, add to label, encrypt with private key), then it can be decrypted and the original hash can be compared with the computed hash from the printed label. For example, a sample of or the entire Iriscode™ template could be used for the hash generation. The integrity of the label and the authenticity of the sender can thus be verified based on the results of the comparison.

In addition, the method can include obtaining an image of an iris of at least one eye of one or more shippers at a destination responsible for the movement of the goods between the sender and the receiver, and storing identity information relating to the shippers in a transactions database. Preferably, the information comprising the IriStrip™ data is encrypted to further enhance the security of the shipping transaction. The IriStrip™ data has a template of an image of an iris which can be used to authenticate the proposed/claimed identity of a person involved in the shipping transaction, or can be used to identify a person involved in the shipping transaction by comparing an obtained iris image to stored iris images.

The present invention can minimize and/or eliminate altogether fraud or theft associated with certain special handling areas. The system and method of unified tracking, by scanning the IriStrip™ data of a package thereby reading a stored IrisCode™ template therein and capturing an iris image of each person involved in the shipping process, can include persons responsible for providing high-value packages into and retrieving packages from these special protection areas. One template, including the IrisCode™ in an IriStrip™ data, can be responsible for tracking all packages. The invention provides a unified security monitoring system using this one template approach to manage accountability and authorization of access to secure packages and facilities, as well as, the information related to each secure package.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other aspects of the present invention will become apparent from the following detailed description of the invention when considered in conjunction with the accompanying drawings. For the purpose of illustrating the invention, there is shown in the drawings an embodiment that is presently preferred, it being understood, however, that the invention is not limited to the specific methods and instrumentalities disclosed. In the drawings:

Figure 1 is a schematic diagram of an exemplary system for sender/receiver authentication using iris recognition and encryption in accordance with the present invention;

Figure 2 is a flowchart illustrating an exemplary iris enrollment process;

Figure 3 is a schematic diagram of another exemplary system for sender/receiver authentication using iris recognition in accordance with the present invention;

Figure 4A is a schematic diagram showing an exemplary 2-D bar code having printable and readable biometric data in accordance with the present invention;

Figure 4B is a schematic diagram showing an exemplary IriStrip™ data structure having printable and readable biometric data in accordance with the present invention;

Figure 5 is a schematic diagram showing an exemplary label having IriStrip™ data disposed on a package in accordance with the present invention;

Figure 6 is a schematic diagram showing an exemplary reader device and IriStrip™ data structure in accordance with the present invention;

Figure 7 is a schematic diagram showing an exemplary imaging device in accordance with the present invention;

Figure 8A is a schematic diagram showing an exemplary controller in accordance with the present invention;

Figure 8B is a schematic diagram showing another exemplary controller in accordance with the present invention;

Figure 9 is a flowchart of an exemplary secure shipping process in accordance with the present invention;

Figure 10 is a flowchart of another exemplary secure shipping process in accordance with the present invention; and

Figure 11 is a flowchart of another exemplary secure shipping process in accordance with the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention is directed to a system and method for secure shipping transactions using iris recognition. The system and method provide for secure shipping transactions by authenticating the claimed identity of one or more persons involved in the shipping transaction and/or identifying one or more persons in the shipping transaction. The system and method use iris patterns as a means of authenticating the identity thereby ensuring a secure shipping transaction. Identification information relating to one or more of the sender, the receiver, and a shipper involved in the shipment of a package, or document, can be printed in one or more strips having printable and readable data that can be affixed to the package

during transit. When the package reaches its destination, the information contained in the printable and readable data is read and compared to a captured iris image to authenticate one of the shipper at a particular (e.g., intermediate) destination and the receiver at the final destination, and can also be compared to stored iris images in a database to authenticate the identity of the sender. In addition, the security and privacy of the persons involved in the shipping transaction can be protected using authorized cryptology techniques.

As shown in Figure 1, the system 10 the present invention includes an iris imaging device 11 and an input device 12, such as a keyboard or mouse, and the appropriate software for enrolling applicants in an application by capturing an iris image and, optionally, other identification data.

Referring to Figure 2, the steps which comprise an exemplary iris enrollment process 40 are illustrated. The data collection step includes acquisition of a high-quality iris image using a suitable imaging platform, at step 41. Typically this platform will utilize low-level infrared illumination and an infrared-sensitive camera. The resulting image is processed to extract a digital code, such as for example, a fixed-length 512-byte digital code, at step 42, that fully captures the unique information used for identification. The IrisCode™ record is stored, at step 43, in a database along with other personal information that has particular value for the specific identification application. Other identification information can be entered at step 44 and might include, a graphical representation of the person's signature, the person's name, a face picture of the individual, an ID number, address, telephone number, for example.

The enrollment of individuals can be accomplished by, for example, a shipper at a fixed location, shippers' employees at remote or mobile locations, and a third party which provides shippers with a database of people and their authorization.

Referring back to Figure 1, the system includes a database 13, or memory, for storing the enrolled iris images and other identification information. The system 10 includes a printer device 14 for printing printable and readable data 15 having one or more stored iris images. The printable and readable data 15 can be printed on, for example, a label 16 which can be attached to a package 17, or document, to be shipped. The system 10 includes a reader device 18 for reading the printable and readable data 15 at a N^{th} destination along the shipping route. The same or another iris imaging device 11 can be used at each N^{th} destination for capturing an iris image of one or more persons involved in the shipping transaction. The

system 10 also includes at least one processor 19 having a memory 20 for authenticating the security of the shipping transaction based on a comparison of a captured iris image to a stored iris image in the printable and readable data 15, or alternatively, the database 13. The label printer device 14, handheld iris imaging device 11, and optical character reader device 18 can be included in one unit, or alternatively, they can each comprise a separate device.

As shown in the exemplary system of Figure 3, the present invention can include technologies for iris recognition 11, public/private key encryption 21, and message digest functions 22 in a system and method for assuring the safe delivery of, for example, sensitive, classified, proprietary, or high value shipments to the intended recipient. A template (hereinafter also referred to as an "IrisCode™" template) is extracted from the captured iris image and is a unique, commensurable, and compact digital biometric code generated from the iris of the eye that remains unique to the individual. The IrisCode™ templates can be printed as sequences of numbers, characters, indicia, or other spatial patterns by the printer device 14 as part of the printable and readable data 15. Preferably, the printable and readable data 15 (herein after also referred to as IriStrip™ data) comprises an encrypted, printable and readable code. The IriStrip™ data 15 can be read by the reader device 18 that reads the printed IrisCode™ template, much the same way that Universal Product Codes (U.P.C.'s) are read on products in supermarkets.

In addition, because the IrisCode™ template has a compact, standard form, it can be printed as a series of indicia in the IriStrip™ 15 data on, for example, a shipping label 16, or a tag, a card, etc. The printed format can be binary, octal, or hexadecimal characters, or any other format which uniquely expresses digital data. Because the IrisCode™ template constitutes a unique message, its integrity can be protected using a message digest function 22 ("hashing" function) in much the same way that digital messages are protected.

Furthermore, the system 10 can also include an encryption device 21, as shown in Figure 3. In this embodiment, the biometric template is encrypted using an encryption device 21 so that the output is an encrypted biometric template that can be used by the printer 18 in printing the printable and readable data 15. Encryption can be with any of the known encryption techniques using public and private keys to encipher and decipher the data, respectively. The existing public/private key infrastructure which has been developed for secure electronic transactions and messaging can be used to authenticate the sender through

the creation of a printed digital signature which can be incorporated into, for example, the return address of the sender. Together with the encryption technologies, IrisCode™ templates provide a means for accurate, reliable, unique identification of a sender and/or a receiver in a shipping transaction. One advantage offered by this embodiment of the invention is the security of shipping transactions which utilize the biometric template is enhanced because the data is generated and encrypted and thus is less susceptible to theft, alteration, or interception. This is due in part because less people will be aware of the sender's name and address and the receiver's name and address because they are obscured in the IriStrip™ data.

As shown in Figure 4A, the printable and readable data 15 is preferably encrypted as the indicia 25 of a 2-D printable and readable bar code 26 that includes one or more data fields having a number of different data types. For example, as shown in Figure 4B, the printable and readable data 15 can include multiple data fields, including biometric data 15a, graphics data 15b, text data 15c, other data 15d, and a hash of the printable and readable data 15e, for example. The 2-D bar code is a complete data record containing, for example, data, text, graphics, and biometrics that can be immediately applied to an application transaction, without accessing an external database, simply by scanning the symbol. Preferably, the printable and readable data 15 includes identification and tracking information relating to one or more persons involved in the shipping transaction, as well as optional information relating to the package being shipped.

The IriStrip™ data 15 can be printed directly on the package, or preferably, is printed on a label 16, such as a pallet label, a package label, tags, ID cards, etc. As shown in Figure 5, the label 16 can include other information 24 in addition to the IriStrip™ data 15, such as text, sequence numbers, check boxes, lines and pictures, and a variety of shapes and OLE objects. Each label 16 can include one or more data fields 23 for the printing of information. For example, the IriStrip™ data 15 may be printed in one field 23a of a label 16, and address information 24 may be printed in another field 23b of the label 16. The label 16 includes a mechanism (not shown) for attaching the label 16 to the package 17, such an adhesive material, a bonding material, tape, glue, a tie, a string, etc. Multiple labels 16, or pages may be used for the shipping data. For example, two labels 16 may be used, as shown in Figure 5, one label 16a having data relating to the receiver, and another label 16b having data relating to the sender.

Preferably, the system includes a database 13 containing stored identification information for persons enrolled in a particular application. The database 13 allows sorting and selection of stored records for printing. For example, the database 13 can include stored IrisCode™ templates, as well as other optional identification and shipping information, such as name, address, telephone number, etc. of a person. Preferably, the database 13 is a central database maintained and controlled by a central authority, such as a shipper, or third party.

The printer device 14 is adapted to print the IriStrip™ data 15 either directly on a package 17, or preferably the printer prints the IriStrip™ data 15 on a label 16 that can be affixed to the package 17. The printer device 14 can include any standard printer device, including thermal transfer, laser, print and apply, and impact printer technologies. Printers 14 that are suitable for use with the present invention include, for example, printers manufactured by the following companies: ATC, Avery, C. Itoh, Datamax/Fargo, Data South, Decision Data, Eltron, Esselte Meto, Facit, Genicom, Intermec, IBI, IBM, Inducomp, Mannesman Talley, Monarch, Novexx, Printronix, Paxar, Printek, RJS, Sato, Standard Register, Superior Machine, TEC, Tharo, Willet, Zebra. The printer 14 can be connected to the system 10 using any conventional wire or wireless connection technique, including COM and LPT.

Preferably, the system 10 includes a software program (not shown) for the development, printing, and reading of the IriStrip™ data 15 that is user-friendly and flexible. The software is preferably compatible with most operating systems, such as Windows 3.11/95/98/NT/2000. The operating system can include simple customized screens for simple entry of identification data and manipulation of system devices. The software is preferably adapted for a dedicated use for printing and reading of one or more standard label formats (e.g., one standard format for the address label and another standard format for the return address label). However, the software is preferably flexible to allow the user to change the design of the label as required.

The software preferably supports most popular label printers from impact printers through thermal transfer, print and apply, and laser printer technologies. The software can include any standard labeling software, including labeling software manufactured by T.L. Ashford, Strandware, Inc., Electronic Imaging Materials, Inc., for example. The software preferably provides for easy integration of the labeling process into shippers' systems and

programs (e.g., such as RPG, CL and COBOL) and existing database files. The software should allow the user to specify label formats, define fields, and merge fields with other identifying data. Although the system preferably uses 2D bar code symbology, the software preferably is capable of supporting other popular bar code symbologies including UCC 128, Interleave 2 of 5, EAN, UPC, Postnet, CODE 128, CODE 39, Maxicode, CODABAR, MSI, CODE 93, for example.

As shown in Figure 6, the reader device 18 is adapted to read or scan the IriStrip™ data 15 and extract various information contained therein. The reader device 18 can be a contact type reader (not shown) or a non-contact type reader, as shown in Figure 6, having a predetermined read zone and bar size range as determined by the particular application and reader device. The reader device 18 can be either a fixed mounted or a handheld device. The reader 18 can be connected to the system 10 using any conventional wire or wireless connection technique. The reader 18 can be powered from any standard power supply, such as external wall power or internal battery power. Preferably, the reader 18 is a lightweight, ruggedized, wireless, battery operated, handheld 2-D bar code laser scanning device, such as those manufactured by SUNMAX Bar Code Solutions of El Monte, CA.

As shown in Figure 7, an exemplary imaging device 11 comprises an iris acquisition device 105, an imaging lens 110, a mirror 120, an optional diopter correction lens 125, and an illuminator 130. The imaging device 11 can be a fixed, or preferably a portable device. The imager 11 can be powered by a standard DC or AC supply, and preferably a 9-volt battery (not shown). The imaging device 11 can be connected to the system using any conventional wire or wireless connection technique.

The system 10 includes one or more imaging devices 11. For example, the system 10 can include an imaging device at the database having the stored IrisCode™ templates, an imaging device at the transactions database, an imaging device 11 at each of the sender's location and the receiver's location, and at each destination N in the shipping process. Alternatively, a single portable imaging device 11 can be used by, for example, the shipper's employee wherein the imaging device 11 follows the package 17 as the employee travels from one destination N to another. The number of location of the imaging device or devices 11 is such that each transaction in the shipping process is captured and recorded.

The iris is a protected internal organ that is, at the same time, readily available for outside observation. Its complex textural pattern of striations, crypts, rings, furrows, etc., has extremely high information content, yet is stable from about the age of one year throughout life. Notably, the iris structures are formed with minimal genetic penetrance (e.g., they are not influenced by the individual's genetic make-up) and so are dramatically different for every individual and indeed for every eye. If the variability inherent in the iris is expressed in statistical terms as the number of independent degrees of freedom, or forms of variability across individuals, the estimated number of such degrees of freedom is 266. This high information content, extracted by sophisticated computer image processing algorithms, enables an extremely accurate and sensitive personal identification technology. One recent study yielded an estimated crossover error rate of 1 in 1.2 million. This value represents the odds of a False Accept (incorrectly identifying a user as someone else) or a False Reject (failing to recognize a valid user), assuming that the system parameters are adjusted so that either type of error is equally likely.

An exemplary imager that can be used with the present invention is a compact, handheld imaging apparatus manufactured by IriScan, Inc. of Marlton, NJ, and has sensors and indicators which assist the human operator in aligning and focusing the device. The imager also automatically captures the image when proper positioning is achieved. Because it is small and compact, it is practical for use as an accessory to a personal computer, and for many business and consumer applications where cost is critical.

Referring back to Figure 7, illustrated is a preferred embodiment of the handheld imager 11 that can be used with the present invention. Any known technique for capturing the iris image can be used, such as those described in Patent Application serial No. 09/200,214 (Attorney Docket No. ICAN-0064), entitled "Handheld Iris Imaging Apparatus and Method", filed on November 25, 1998, which is herein incorporated by reference. The exemplary handheld, non-invasive, non-contacting iris imager comprises iris acquisition device 105, an imaging lens 110, a mirror 120, an optional diopter correction lens 125, and an illuminator 130.

The imager 11 acquires images of an iris with sufficient clarity, focus, and size for use with conventional image processing and comparison routines. A preferred image processing and comparison routine is described in U.S. Patent No. 5,291,560, "Biometric

Personal Identification System Based on Iris Analysis", issued to Daugman, and commonly assigned with the present invention to IriScan Inc., and incorporated herein by reference. However, any processing and comparison technique can be used with the image that is acquired at the imager, such as the image pixel correlation technique described in U.S. Patent No. 5,572,596, "Automated, Non-Invasive Iris Recognition System and Method", issued to Wildes et al. and the techniques described in U.S. Patent No. 4,641,349, "Iris Recognition System", issued to Flom et al., both of which are incorporated herein by reference.

The image processing consists of a number of image processing steps (such as those described in U.S. Patent No. 5,291,560 and U.S. Patent No. 5,572,596, which are herein incorporated by reference) which lead to extraction of a unique and highly specific digital biometric template that can be used to identify the individual based on intensity patterns within the iris. The biometric template is then compared against other templates or images stored in a central database 13 or in another memory, such as the RAM 33 or EPROM 34 within the computer 30, shown in Figure 8A. The database 13, or memory, stores selected data representing images of the iris of a plurality of subjects enrolled in a particular application. A match of the biometric template with a stored template identifies the subject whose iris is being imaged.

As shown in Figures 8A and 8B, the processor 19 is preferably integrated into an operating system that can control the printer, reader, and the imager, and contains the labeling software. The processor 19 can perform comparison, tracking, and other processing functions. Preferably, the printer 14, the reader 18, and the imager 11 can follow one or more protocols as defined by the processor 19.

As shown in Figures 8A and 8B, the processor 19 can reside in a conventional computer 30, such as a standard personal computer, which can comprise the processor 19 (e.g., 100 MHZ, 32 Mbyte DRAM, monitor, keyboard, ports, hard drive, floppy drive, CD-ROM drive). Alternatively, a separate microprocessor (not shown) can reside within each of the printer device 14, the reader device 18, and the imaging device 11 for controlling the functions of the particular device and for interacting with the other devices.

As shown in Figure 8A, the processor 19 can be coupled to the other devices via conventional cables and/or printed circuit boards (PCBs) that can be connected into slots on the computer, such as an ISA slot or a PCI slot. Other conventional means for coupling

the devices to the processor can be employed, such as a standard wireless connection, as shown in Figure 8B.

The processor 19 preferably communicates with the other devices, controls the operation of the other devices, and runs the software which can be held in read only memory (ROM) 31. The processor 19 can be connected via a bus 32 to the ROM 31, a random access memory (RAM) 33, another memory such as an erasable programmable ROM (EPROM) 34, and an input/output (I/O) controller 35. The RAM 33 is large enough to hold at multiple protocols and person/package identification data. The I/O controller 35 is connected to the appropriate circuitry and drivers (not shown) for issuing commands and instructions to the different devices.

Figure 9 is a flowchart illustrating one exemplary embodiment of the invention, which provides for authentication of one or more of the sender and receiver, and also for protection of the person's iris template (e.g., the IrisCode™ template) while the shipment is in transit. As shown in Figure 9, the system includes a database of iris templates obtained through enrollment of valid recipients (and others involved in the shipping transaction, such as shippers, carriers, and senders) for a particular application, at step 300. The database can be set up to allow access to authorized users only, such as a system administrator, shippers and carriers involved in the shipping transaction. Preferably, the database is protected at a high level from unauthorized access by a security system or wall, such as, for example, a PCIris™ device. The database can be maintained by any of the persons involved in the shipping transaction, such as the sender, the receiver, or a shipper, or alternatively, the database can be maintained by an outside third party not otherwise involved in the shipping transaction (e.g., a system administrator).

Printable and readable data including biometric data in the form of, for example, a shipping label, is attached to the package or shipment, at step 315. Preferably the label is composed of multiple parts, such as for example, the sender identification and the recipient identification. To form the recipient identification, the shipper extracts the recipient's iris template (e.g., the IrisCode™ template) from the database and encrypts it, at step 305, using one of a number of suitable symmetric encryption techniques and a session key generated, at step 307 preferably using well-known techniques. The encrypted IrisCode™

template is printed on the label, at step 310, along with the recipient's name, address, and if desired, a tracking number or other unique shipping number generated by the carrier.

To form the sender identification, the recipient's IrisCode™ template is processed using a message digest function to generate a "hash", at step 320. The hash, sometimes called a checksum or message digest, is a unique, fixed-length digital value that can be computed for any data structure, but from which the contents of the data structure cannot be reconstructed, (e.g., it operates one-way only). It has the property that any change in the data structure, large or small, produces a significant and easily detected change in the hash. Standard hash techniques that can be used with the present invention include MD4, MD5, and SHA (Secure Hash Algorithm). The hash generated at step 320 is a unique but very compact summary of the IrisCode™ template. The hashing function is preferably one-way and reproducible, so that if the IrisCode™ template is modified in any way its hash will change dramatically. This provides a means of protecting the integrity of the template.

The hash of the IrisCode™ template is combined with the session key used to encrypt the IrisCode™ template, at step 321 and, if desired, other sender information, such as name and address. These combined data are then encrypted, also at step 321, using the sender's private key, provided at step 323, and a suitable asymmetric encryption technique is used to form a digital signature, unique to the sender, which can be printed on the shipper identification part of the label, at step 325 and attached to the package at step 315.

When the shipment is delivered to a particular destination (e.g., the Nth destination), at step 330, the carrier, or shipper, uses the sender's public key, provided at step 333, to decrypt the digital signature and recover the hash and the session key, at step 335. The session key is then used to decrypt the printed IrisCode™ template, at step 340. The recipient's eye is imaged and the IrisCode™ template is extracted, at step 345, and compared against the IrisCode™ template printed on the shipment at step 350. If a successful match occurs, the recipient is authenticated, at step 355, and the package is delivered to the validated person. If a match is not made, then the recipient is invalidated at step 360, and the package is not delivered.

The hash from the decrypted printed IrisCode™ template is re-computed, at step 365, and compared, at step 370, to the hash contained in the digital signature. If they match then the integrity of the printed IrisCode™ template is verified, as is the authenticity

of the sender, at step 375. If they do not match, then the authenticity of the sender is invalidated at step 380.

Preferably, every step in the process is recorded in a database, such as a transactions database, at step 385. The transactions database provides a record of the transactions involved in the shipping process and provides an audit trail of accountability that is recorded and archived as appropriate. The transactions database can comprise a separate database or the same database that stores the IrisCode™ templates. Preferably, the transactions are hashed just prior to storage on the transaction database. Exemplary transactions include, acceptance of a package by the shipper and capture of the sender's IrisCode™ template, delivery to various parts of the shipping chain, handling of the package by shipper employees IrisCode™ and capture of employee's iris images for employees who have accepted physical custody of a package, who have handled a package, or have placed a package in a secure storage facility, the acceptance/delivery of the package at its final destination, etc.

The encryption of the IrisCode™ template is optional and is not a requirement of the system and method. The IrisCode™ template is preferably encrypted prior to printing it on the label in order to prevent it from being copied and used for an unauthorized shipment or some other impersonation of the sender. If the carrier can guarantee the security of the printed IrisCode™ template without depending on encryption, the embodiment of the invention shown in Figure 10 can be used.

As shown in the flowchart of Figure 10, in another exemplary system, the recipient IrisCode™ template can be printed directly on the shipment without encryption. A database containing stored IrisCode™ templates is provided at step 400. An IrisCode™ template of the intended recipient is obtained from the database and a hash is computed for the IrisCode™ template, at step 405, and incorporated into a digital signature that is encrypted, at step 410, with the sender's private key, provided at step 415. The encrypted digital signature is then printed onto, for example a label, at step 420, and the label is attached to a package or document to be shipped, at step 425. An address label is also printed having the IrisCode™ template, at step 430, and attached to the package, at step 425.

The package is shipped to the intended recipient and when the shipment is delivered, at step 435, the carrier scans the IrisCode™ template from the label, at step 440,

and compares it, at step 450, to the recipient's "live" IrisCode™ template, obtained at step 445, before releasing the shipment to the valid recipient, at step 455. If the obtained IrisCode™ template does not match the scanned IrisCode™ template read off of the label, at step 440, then the recipient is invalid and the carrier does not deliver the package, at step 460.

Once the recipient has been authenticated, at step 455, he can read, or scan the digital signature, at step 465, and decrypt the digital signature, at step 470, using the sender public key provided at step 475. The original hash, step 470, is then compared with that computed hash, step 477, from the printed label, at step 480, to verify the integrity of the label and the authenticity of the sender. If a match is found, then the signature is valid and the sender is authenticated at step 485. If a match is not made, then the signature is invalidated at step 490.

As shown in Figure 10, every step in the process is preferably recorded in a database, such as a transaction database, at step 495. The transaction database provides a record of the transactions involved in the shipping process and provides an audit trail of accountability that is recorded and archived as appropriate.

Figure 11 shows an exemplary method for secure shipping using iris recognition and encryption in accordance with the present invention and addresses certain additional shipping security risks not treated by the two previous embodiments, shown in Figure 9 and Figure 10. As shown in Figure 11, a shipping request is generated at step 500. The shipping request from the sender lists codes known to the shipper, such as, for example, the names of the sender and receiver, the value of the goods, the identity of an insurer who will provide loss coverage while the package is in transit, the IrisCode™ template of one or more persons involved in the shipping transaction, etc. Based on the coded identity of the sender, the shipping company picks up the package and captures the IrisCode™ template of the sender, at step 505. The system generates routing information at step 510, including for example, sender and receiver data, such as identification codes, iris templates, addresses, etc. Route generating data can be obtained, at step 515, from a database. In addition, the sender's name and address are encrypted with the sender's private key to produce a digital signature authenticating the origin of the package. This encrypted information is printed on a label, at step 520, and affixed to the package, at step 525. Alternatively, the encrypted information can be printed directly on the package or document to be shipped. The sender and receiver

identification codes and the sender's captured IrisCode™ template are encrypted with the shipper's public key and this is also printed on the package.

The shipper or carrier then delivers the package and when the package arrives at a shipper's facility (e.g., the N^{th} destination), at step 530, the shipper reads the labels attached to the package at step 535. The shipper decodes the sender and receiver identification codes and the sender's IrisCode™ template using its private key, at step 540. The IrisCode™ template is compared to the template contained in the shipper's database for that sender. If the sender is authenticated, the shipper generates a routing sequence for the package, specifying the sequence of N destinations (all of which are secure shipper facilities) which the package will pass through on its way to the receiver. Each of these N destinations has a public and private key pair. A label is printed which has one entry for each N destination, consisting of the address or other location information for that destination. The address for the $(N+1)^{st}$ destination is encrypted using the public key of the N^{th} destination, enabling each destination facility to decrypt the address of the next destination and forward the package to that destination without having any other information about the origin or final destination of the package. Further, each destination entry is digitally signed with the router's private key to allow authentication of the routing information.

This digital signature is created by first generating a hash of the destination address and encrypting this hash using the router's private key. This digital signature is added to the destination address and the combined message is encrypted using the destination's public key, as described above. This assures the integrity of the routing information at each step in the package's journey from sender to receiver.

In addition to generating the routing information, the shipper can request, for example, insurance coverage for the full value of the package from an insurance company, agent, or broker, at step 517. After insurance coverage is arranged the agent or broker returns an identifying sequence number to the shipper, at step 518, which certifies existence of the coverage. This may be printed on the package, at step 520, or entered in the shipper's database as part of the tracking information for the package, at step 515. The system can include a billing and insurance interface, such as an LDAP directory with pointers to either the IrisCode™ database or the transactions database.

The processing used at each N destination to forward the package is shown in Figure 11. The first routing label entry is read, at step 535 and decrypted with the N destination's private key, at step 540. The decrypted entry will consist of an address segment (the address of the next destination) and a digital signature segment. The signature portion of the message is extracted and decrypted with the router's public key, at step 545. This decrypted signature is the original hash of the destination entry, and it is compared, at step 550, with a hash generated from the address portion of the routing label entry, provided at step 547.

If the two hashes match, the integrity and authenticity of the address portion are both validated, at step 550. If the hashes do not match the process checks if this is the last entry in the routing information, at step 555. If it is not the last entry, the next entry, step 560, in the routing list is decrypted in the same way. If no authentic entry is found and it is the last entry the package must be returned to the sender, at step 565.

If a valid entry is found, the package is forwarded to the corresponding next N destination, at step 570. If desired, a temporary (plain text) address label for the next destination can be attached to the package to facilitate handling. If it is determined that the next destination is not the last destination in the routing information, at step 575, then the shipper continues with the delivery of the package in accordance with the next set of shipping instructions.

When the package reaches its final destination (e.g., the last entry in the routing list is identified at step 575), the receiver identification code, which has been encrypted as part of the last destination's address, is recovered. This identification code is used to extract the receiver's address and IrisCode™ template from the shipper's data base, at step 515. The address and IrisCode™ template are printed on a delivery label that is attached to the package, at step 580. When the package is delivered, an image of the receiver's iris is captured and the resulting IrisCode™ template is compared with one scanned from the package label, at step 585. If the receiver is authenticated, the package is delivered, at step 590. The receiver may scan the sender's encrypted name and address from the package and decrypt it with the sender's public key, if desired, to authenticate the origin of the package. If the receiver is not authenticated, then the package is retained by the shipper or returned to the sender at step 595.

Other exemplary applications that may benefit from the secure shipping transaction using printable and readable biometric data include:

1. Classified Materials (Nuclear, distribution of encryption keys);
2. Money delivered from a printing agency to a Government;
3. Intellectual Property and Proprietary data;
4. Jewelry; and
5. Consumer items.

In addition, because the iris authentication of sender and receiver adds a significant extra measure of security to the shipping service, the invention results in an economic benefit, such as for example, lower insurance costs to the sender and/or the receiver based on the value of the package to be sent and the reduced risk of theft of fraud.

The present invention can minimize and/or eliminate altogether fraud or theft associated with certain special handling areas. The system and method of unified tracking by scanning the IriStrip™ data of a package and the IrisCode™ template of each person involved in the shipping process, can include persons responsible for providing high-value packages into and retrieving packages from these special protection areas. One template, including the IrisCode™ template in an IriStrip™ data, is responsible for tracking all packages. The invention provides a unified security monitoring system using this one template approach to manage accountability and authorization of access to secure packages and facilities, as well as, the information related to each secure package.

In another embodiment of the present invention, notably in the early enrollment and implementation phases in order to build up the database of IrisCode™ templates, the label may only have the sender's IrisCode™ template. The database can be developed by having, for example, the shipper's employee captures the IrisCode™ template of the sender when he picks up the package. The sender's IrisCode™ template would be printed on the label and entered into the database at the time that the package is picked up, providing the sender was not already enrolled. In addition, at the time the shipper delivers the package to another shipper or the intended receiver, the shipper's employee, for example, would capture that person's live iris image. Preferably, prior to capturing the live iris image, the shipper's employee would ask if the person wanted to be enrolled. If yes, an electronic form, for

example, having a privacy statement and an use authorization would be presented. The "signing" or acknowledgment of the form could be the capturing of the live iris image.

Although illustrated and described herein with reference to certain specific embodiments, it will be understood by those skilled in the art that the invention is not limited to the embodiments specifically disclosed herein. Those skilled in the art also will appreciate that many other variations of the specific embodiments described herein are intended to be within the scope of the invention as defined by the following claims.

What is claimed is:

1. A system for biometric authentication of shipping transactions comprising:

printable and readable biometric data containing at least one stored iris template, said printable and readable biometric data being affixed to a package to be shipped;

an imager for capturing an image of an iris of an eye of a person to form an iris template; and

a comparator for comparing said captured iris template to said at least one stored iris template, wherein an authentication of an identity of said person is based on said comparison.

2. The system according to claim 1, wherein said package is delivered based on said identification

3. The system according to claim 1, wherein said captured iris template is compared to a stored iris template corresponding to a claimed identity of said person in order to verify a secure shipping transaction.

4. The system according to claim 1, wherein said captured biometric template is compared to all of said stored biometric templates in order to verify said secure shipping transaction and to identify said person.

5. The system according to claim 1, further comprising a processor for processing said iris images to extract a template and for performing said comparison.

6. The system according to claim 1, wherein said template is encrypted to protect an identity said person.

7. The system according to claim 6, wherein said encryption is accomplished using one of public-key and private-key technology.

8. The system according to claim 1 further comprising a label which is capable of being affixed to said package, wherein said printable and readable biometric data is printed on said label.

9. The system according to claim 1 further comprising a printer device for printing said printable and readable biometric data.

10. The system according to claim 1 further comprising a reader for reading said printable and readable biometric data and extracting said at least one stored iris image.

11. The system according to claim 1, wherein said printable and readable biometric data comprises indicia of a 2-D bar code.

12. The system according to claim 11, wherein said 2-D bar code further comprises shipping information and handling information relating to said package.

13. The system according to claim 1, further comprising a central database for storing a plurality of enrolled iris templates for a given shipping transaction.

14. A system for authenticating a secure shipping transaction comprising:

a memory for storing a plurality of enrolled iris templates of at least one person involved in a shipping transaction;

a printer device connected to said memory for accessing said enrolled iris templates;

printable and readable biometric data printed by said printer device, wherein said printable and readable biometric data contains at least one of said enrolled iris templates stored therein;

a package having said printable and readable biometric data affixed thereto;

a reader device for reading said printable and readable biometric data and extracting said stored iris template;

an imager device for capturing an image of an iris of at least one eye of at least person involved in said shipping transaction and extracting an iris template from said captured iris image; and

a comparator for comparing said iris template stored in said printable and readable biometric data with said captured iris template for one of authentication of said shipping transaction and identification of said person.

15. The system according to claim 14, wherein said printable and readable biometric data comprises indicia of a 2-D bar code.

16. The system according to claim 14, wherein said comparator comprises a processor responsive to an output of said imager device for comparing said iris template of said captured template with said stored iris template of said printable and readable biometric data.

17. An apparatus for authenticating a secure shipment of a package comprising:

printable and readable biometric data having one or more data fields contained thereon;

at least one biometric trait of at least one authorized person in a shipping transaction, said at least one biometric trait being disposed in one of said one or more data fields; and

wherein said biometric trait comprises an iris template extracted from an iris image captured from an iris of an eye of one of said at least one authorized person.

18. The apparatus according to claim 17, wherein said printable and readable biometric data comprises indicia of a 2-D bar code.

19. The apparatus according to claim 17, wherein said printable and readable biometric data is printed on a label which is affixed to said package to be shipped.

20. The apparatus according to claim 17, further comprising other identification data relating to said at least one authorized person, wherein said other identification data is stored in another of said one or more data fields of said printable and readable biometric data.

21. The apparatus according to claim 17, wherein said printable and readable biometric data further comprises shipping information and handling information relating to said package.

22. A method of biometric authentication of shipping transactions using iris recognition comprising:

generating printable and readable biometric data having at least one stored iris template contained therein;

capturing an iris image of an iris of an eye of a person and extracting an iris template from said captured iris image; and

comparing said captured iris template to said iris template stored in said printable and readable biometric data; and

identifying said person based on said comparison.

23. The method according to claim 22, further comprising authorizing said shipping transaction based on said identification.

24. The method according to claim 22, further comprising printing said printable and readable biometric data on a label, wherein said label is adapted to be affixed to a package.

25. The method according to claim 22, further comprising encrypting said iris template prior to printing said printable and readable biometric data.

26. The method according to claim 25, wherein said encrypting further comprising using public and private keys technologies.

27. The method according to claim 22, further comprising generating a unique digital signature including shipping information using a hashing function, and printing said digital signature on said label.

28. A method of authenticating an identity of a receiver of a package in a shipping transactions using iris recognition comprising:

(a) retrieving an iris template of an intended receiver from a database of stored iris templates;

(b) printing a label having a printable and readable biometric data containing said retrieved iris template of said intended receiver;

(c) attaching said label to said package;

(d) shipping said package from said sender to said receiver;

(e) capturing an image of an iris of an eye of said intended receiver and extracting a iris template from said captured iris image; and

(f) authenticating the security of said shipping transaction based on a comparison of said captured iris template of said receiver to one or more stored iris templates in said printable and readable biometric data.

29. A method of authenticating an identity of a sender of a package in a shipping transactions using iris recognition comprising:

(a) capturing an image of an iris of an eye of a sender of said package and extracting an iris template from said captured iris image; and

(b) verifying an identity of said sender based on a comparison of said captured iris template to one or more iris templates of authorized senders stored in a database.

30. The method of claim 29 further comprising:

(a) printing a second label having a printable and readable biometric data containing said captured iris template of said sender; and

(b) authenticating the security of said shipping transaction once said package has been delivered based on a comparison of said stored iris template of said sender in said

printable and readable biometric data to a plurality of iris templates for authorized senders in a database.

31. A method of authenticating an identity of a shipper of a package in a shipping transactions using iris recognition comprising:

(a) capturing an image of an iris of an eye of one or more shippers involved in said shipment of said package at each N destination and extracting an iris template from said captured iris image;

(b) verifying an identity of each of said shippers based on a comparison of said captured iris template to one or more iris templates of authorized shippers stored in a database;

(c) printing a label at each N destination having a printable and readable biometric data containing an iris template of said authorized shipper at a N+1 destination;

(d) shipping said package to said N+1 destination;

(e) capturing an image of an iris of an eye of one or more shippers involved in said shipment of said package at each N+1 destination and extracting an iris template from said captured iris image;

(f) authenticating the security of said shipping transaction based on each of said comparisons of said stored iris template of said shipper in said printable and readable biometric data to a captured iris template at each N+1 destination; and

(g) repeating steps (a) through (f) until it is determined that said package is at a final destination.

32. The method of claim 31 further comprising storing information relating to each step of said shipping transaction for said package in a transaction database.

33. The method of claim 32 further comprising storing an iris template of each person involved in said shipping transaction in said transaction database.

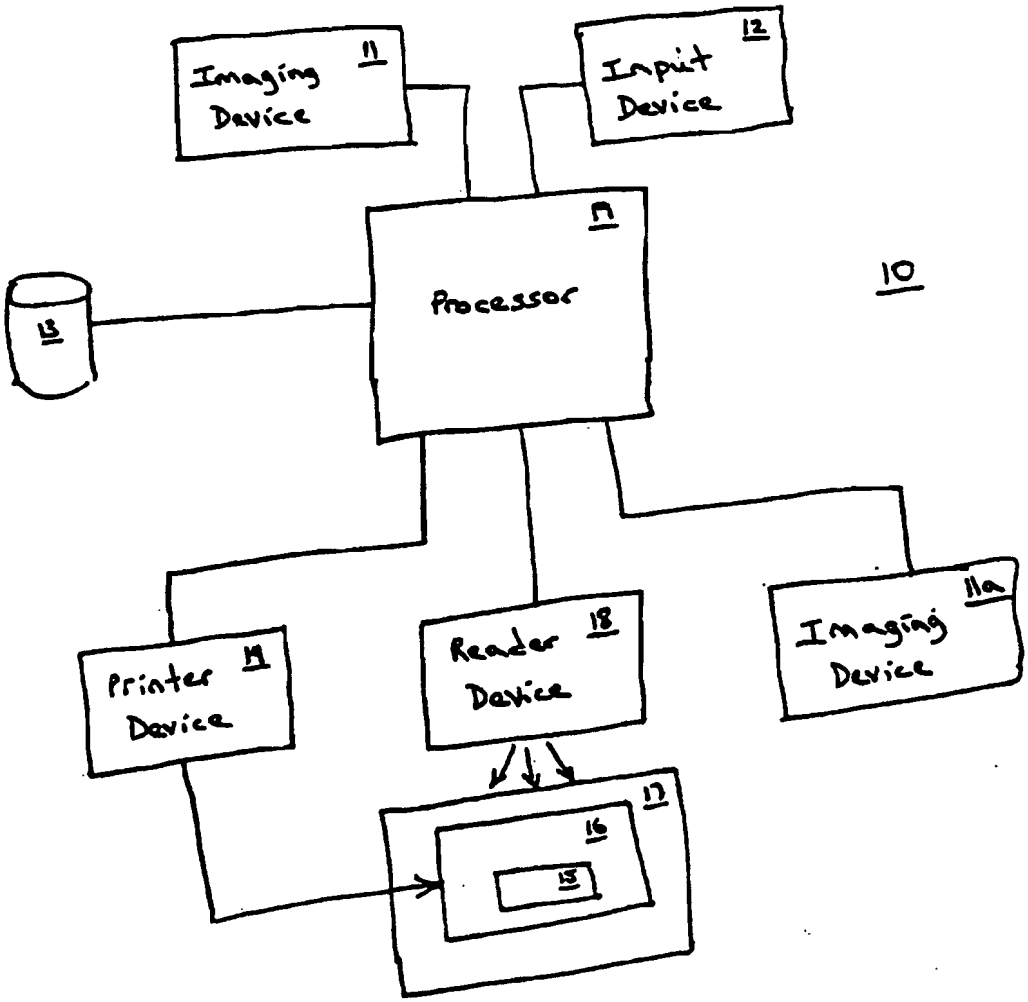

Imaging Device 11
Input Device 12
Processor 11
10
13
Printer Device 14
Reader Device 18
Imaging Device 11a
17
16
15

Figure 1

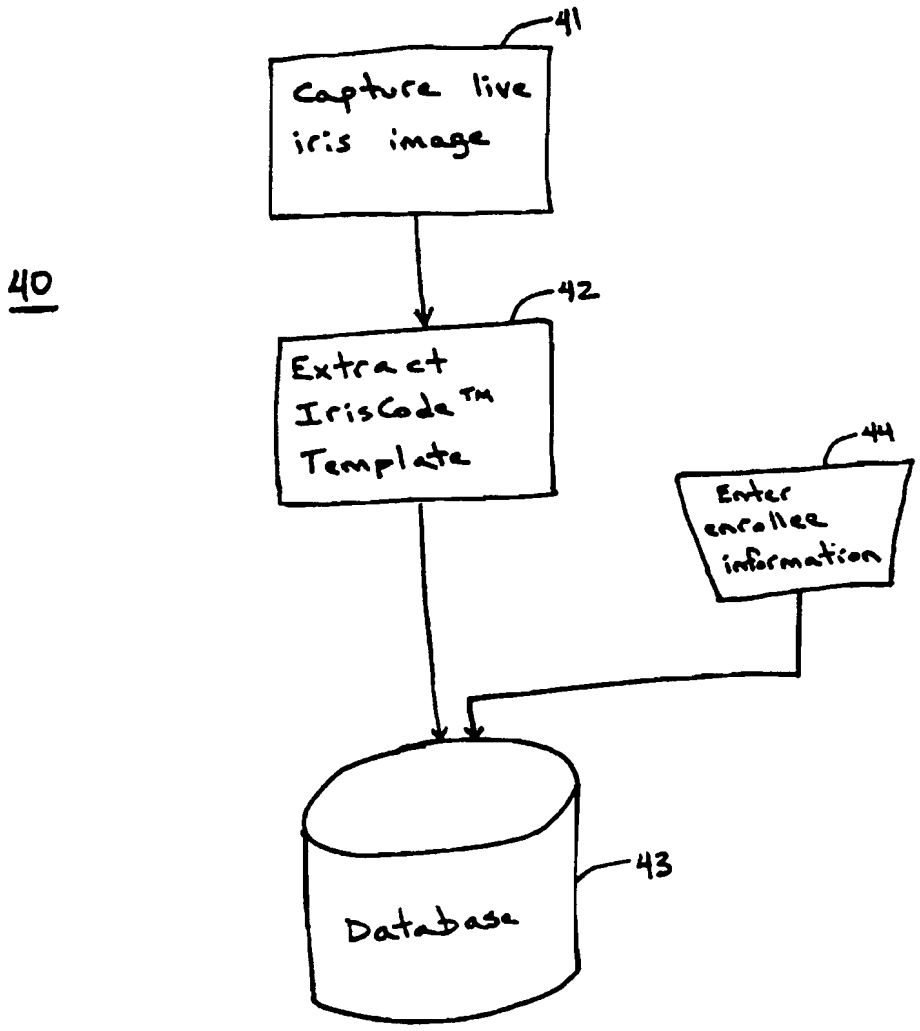

40
41
Capture live iris image
42
Extract IrisCode™ Template
44
Enter enrollee information
43
Database

Figure 2

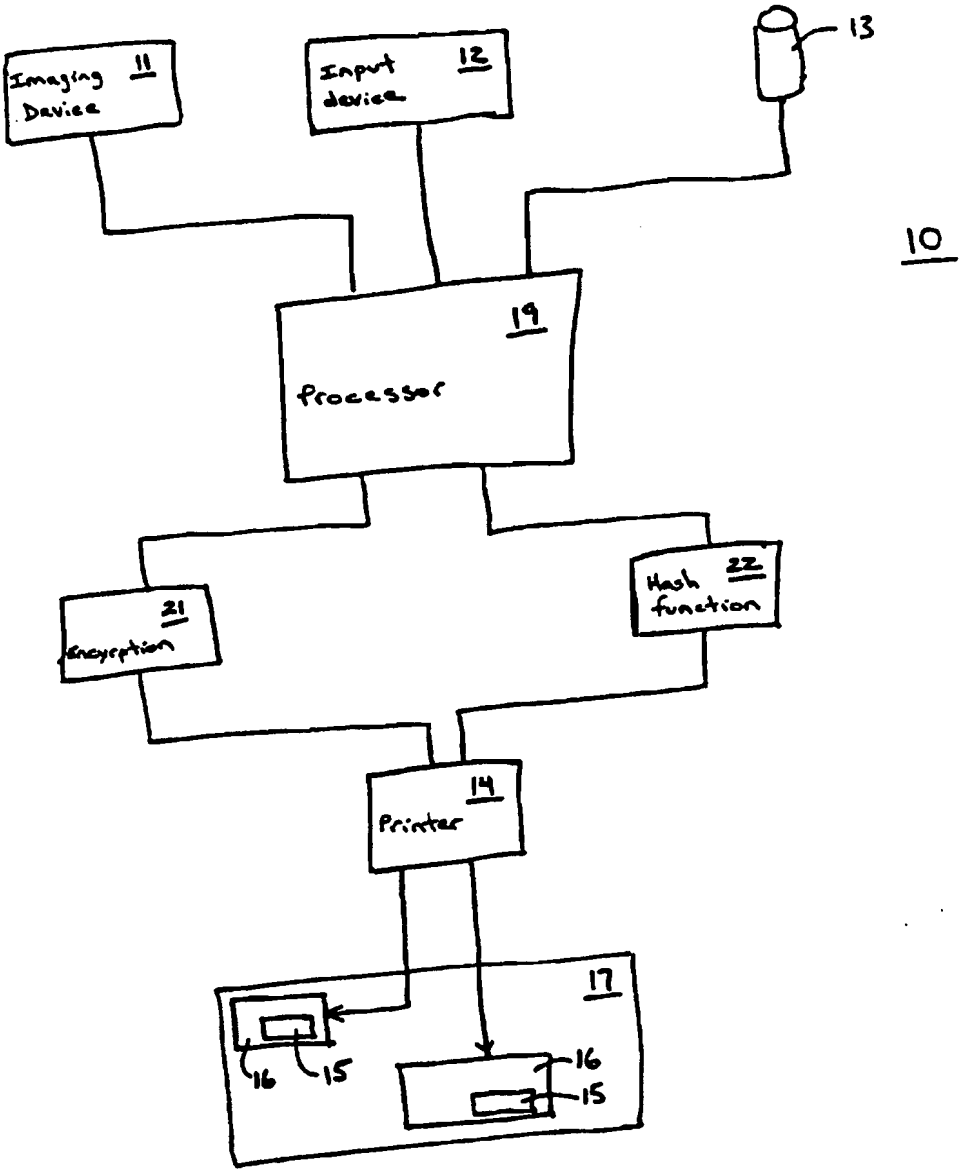

Imaging Device 11
Input device 12
13
10
Processor 19
Encryption 21
Hash function 22
Printer 14
17
16
15
16
15

Figure 3

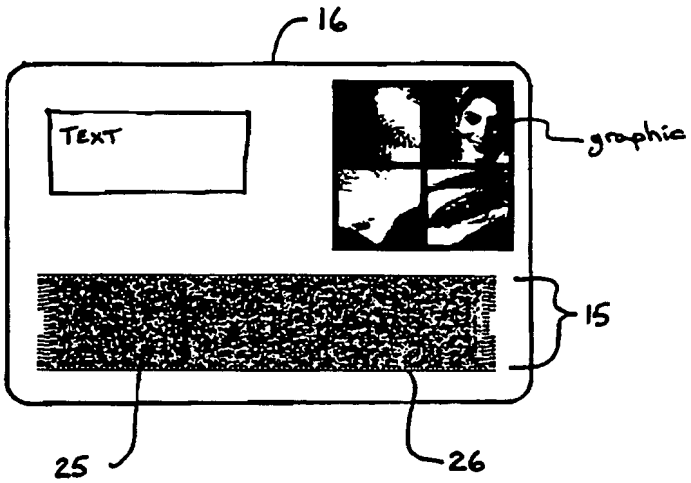


Figure 4A

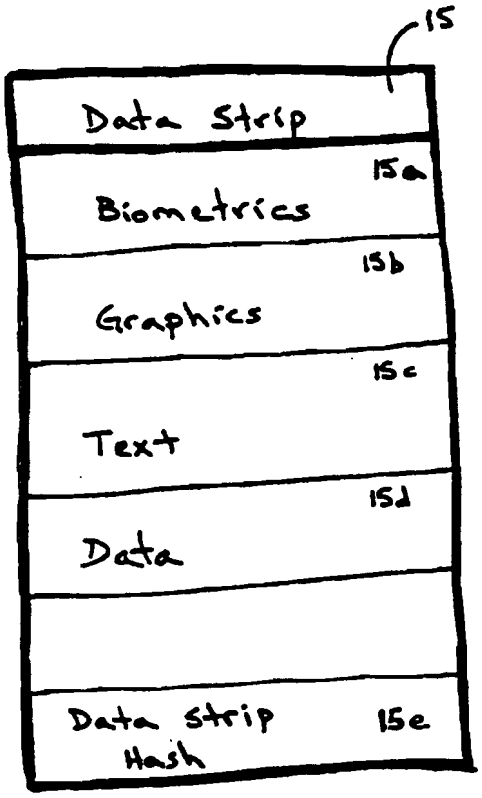

15
Data Strip
15a
Biometrics
15b
Graphics
15c
Text
15d
Data
Data strip Hash
15e

Figure 4B

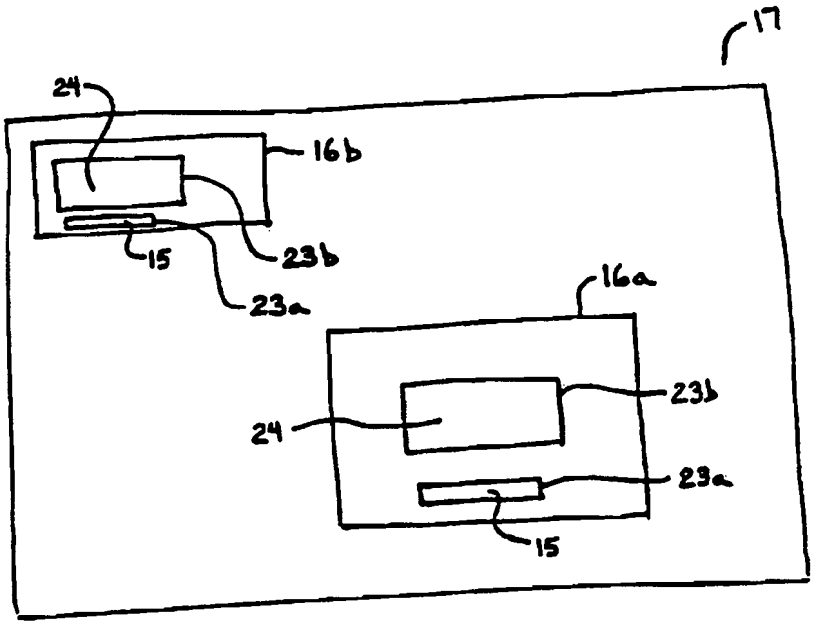


Figure 5

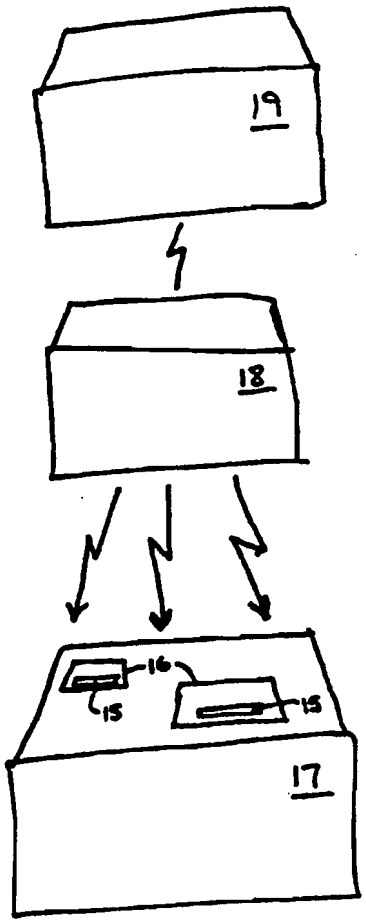


Figure 6

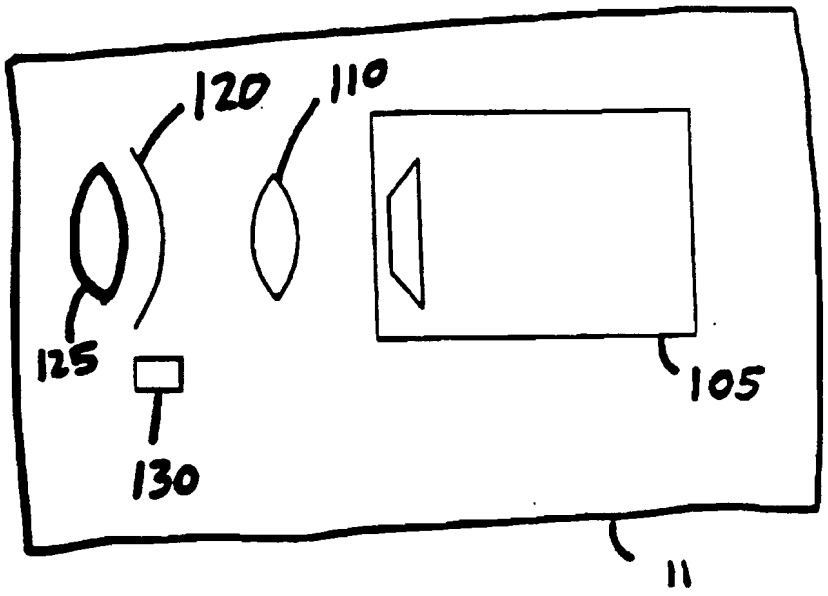


Figure 7

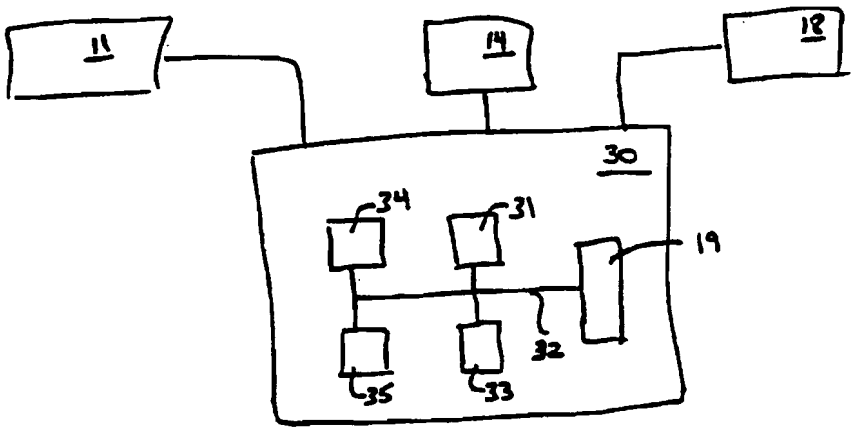


Figure 8A

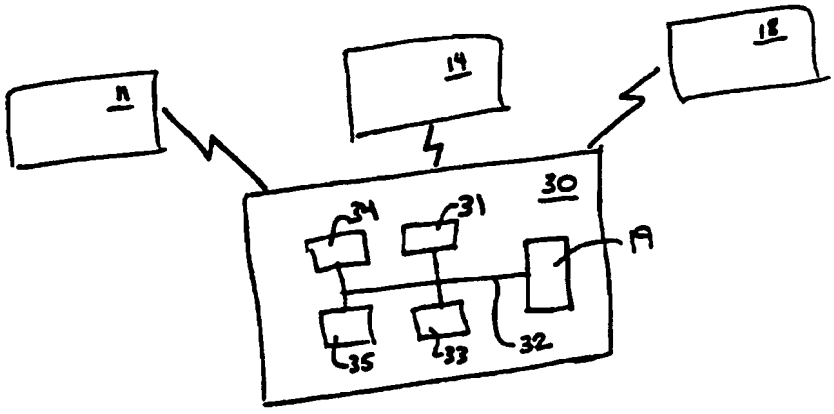


Figure 8B

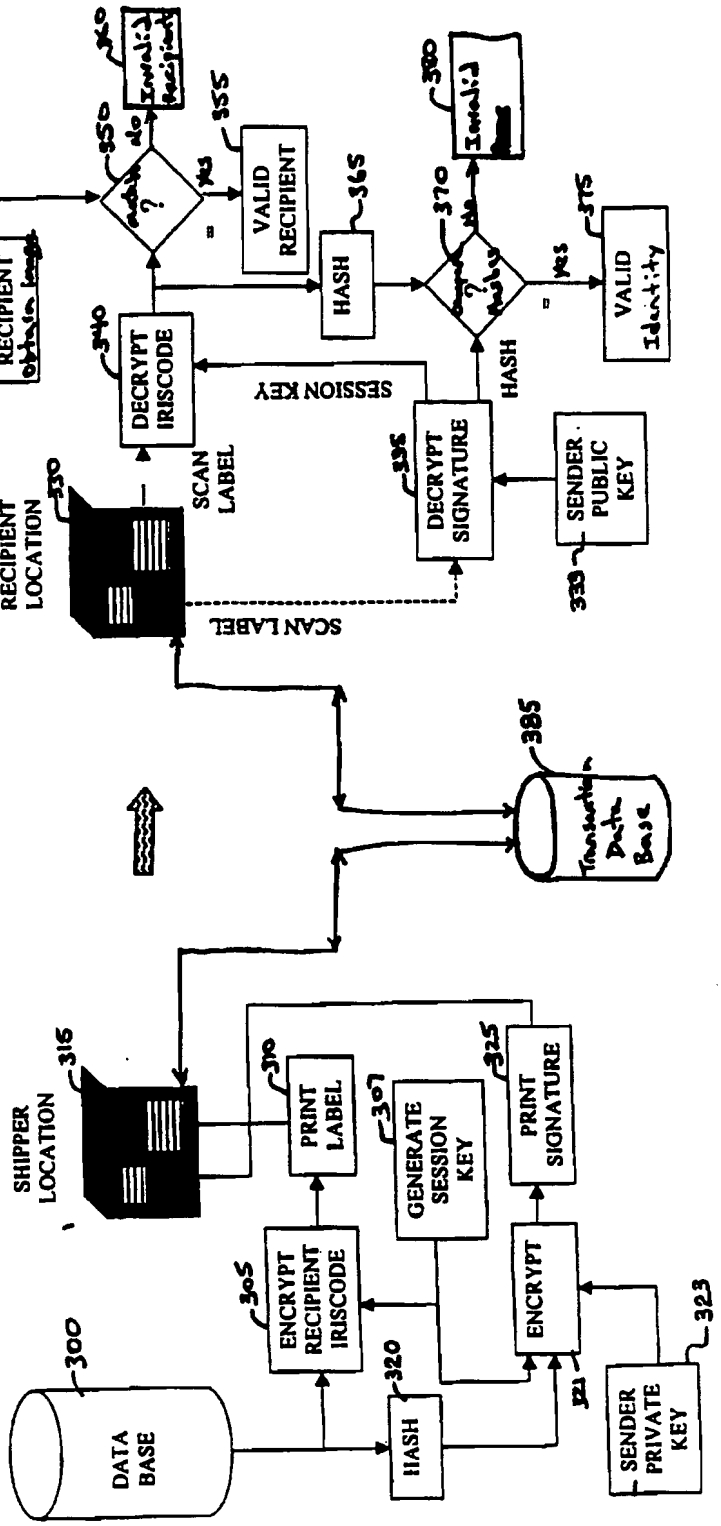

SHIPPER LOCATION
316
DATA BASE
300
ENCRYPT RECIPIENT IRISCODE
305
HASH
320
PRINT LABEL
310
GENERATE SESSION KEY
307
ENCRYPT
321
PRINT SIGNATURE
325
SENDER PRIVATE KEY
323
385
Transaction Data Base
Nth RECIPIENT LOCATION
330
SCAN LABEL
SCAN LABEL
DECRYPT IRISCODE
340
SESSION KEY
DECRYPT SIGNATURE
335
SENDER PUBLIC KEY
333
HASH
SCAN RECIPIENT
345
HASH
365
VALID RECIPIENT
355
VALID Identity
375
Invalid
380
Invalid
360
yes
yes

Figure 9

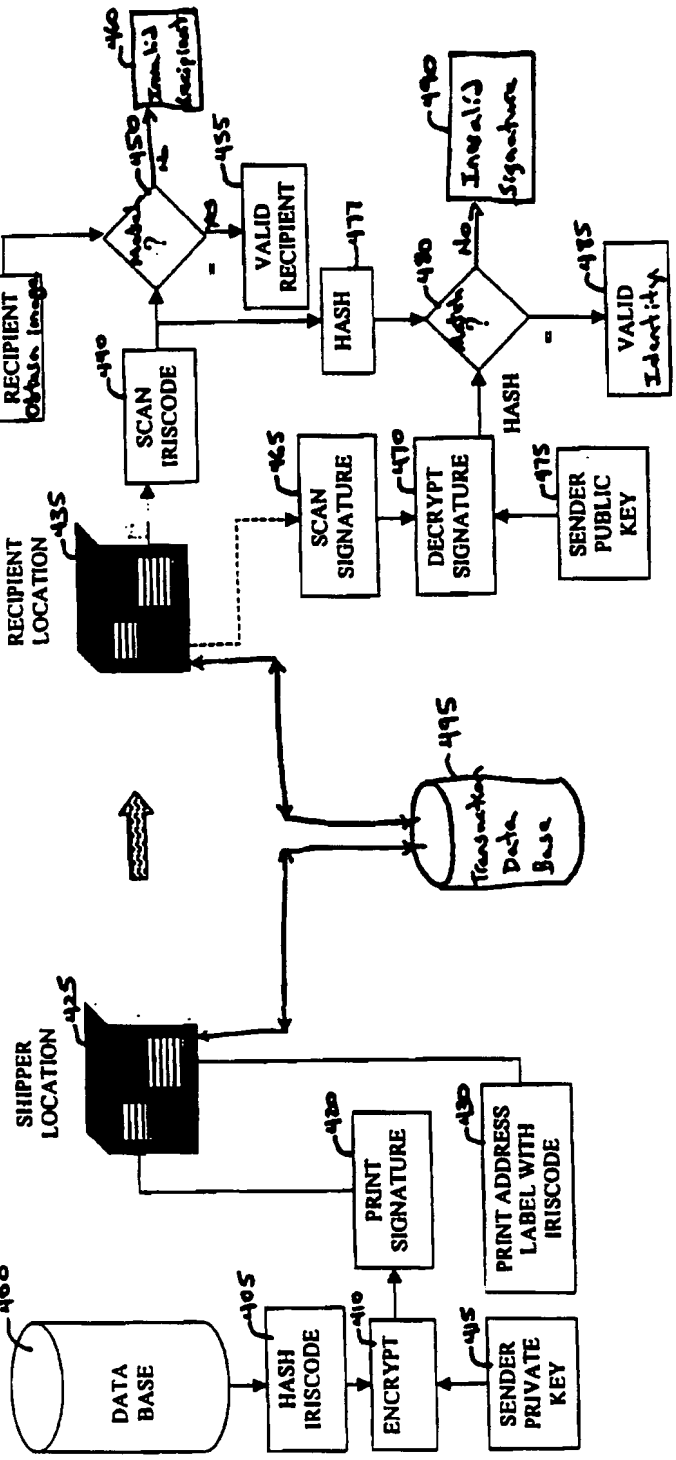

DATA BASE
HASH IRISCODE
ENCRYPT
SENDER PRIVATE KEY
PRINT SIGNATURE
PRINT ADDRESS LABEL WITH IRISCODE
SHIPPER LOCATION
Transaction Data Base
RECIPIENT LOCATION
SCAN IRISCODE
SCAN SIGNATURE
DECRYPT SIGNATURE
SENDER PUBLIC KEY
HASH
SCAN RECIPIENT
HASH
VALID RECIPIENT
Invalid Signature
VALID Identity
Yes
No

Figure 10

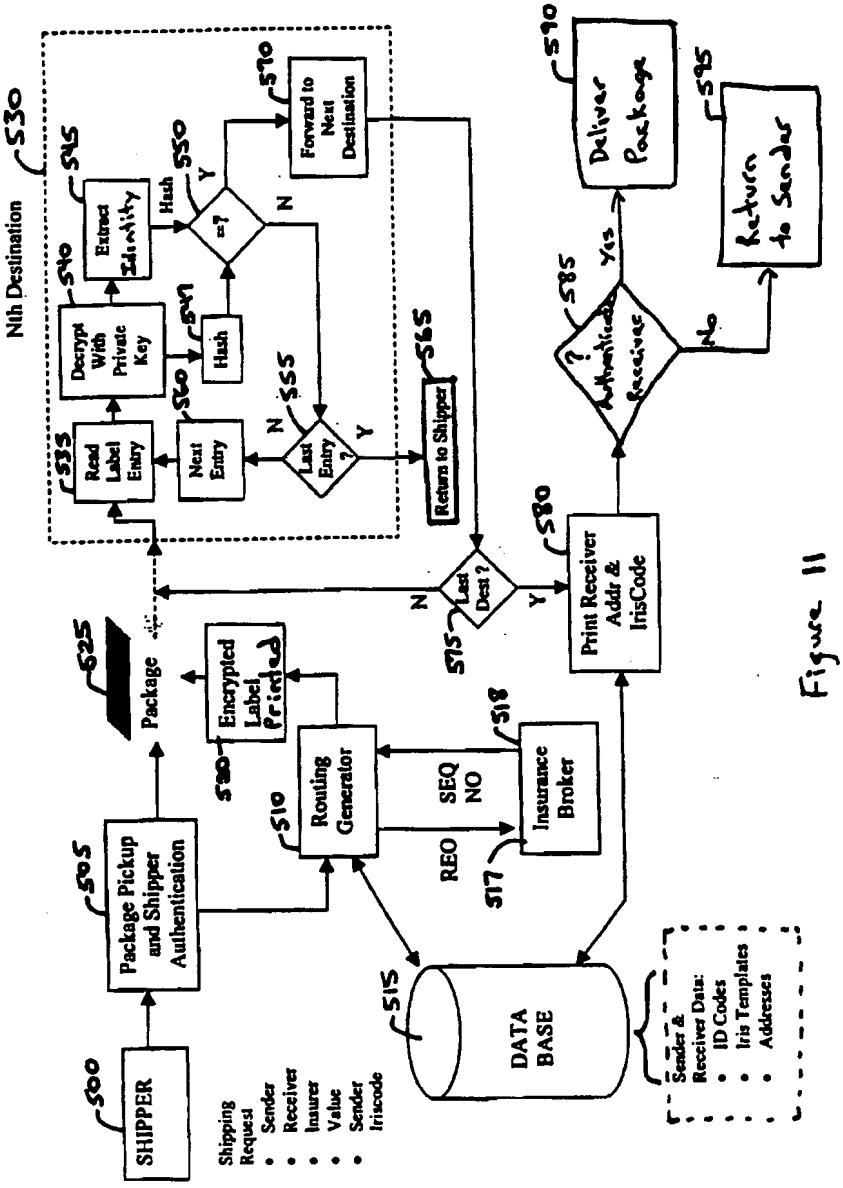

SHIPPER
500
Shipping Request
Sender
Receiver
Insurer
Value
Sender Iriscode
Package Pickup and Shipper Authentication
505
Package
625
Routing Generator
510
Encrypted Label Printed
520
SEQ NO
REQ
517
Insurance Broker
518
DATA BASE
515
Sender & Receiver Data:
ID Codes
Iris Templates
Addresses
Last Dest ?
515
N
Y
Print Receiver Addr & IrisCode
580
Nth Destination
530
Read Label Entry
535
Next Entry
540
Last Entry ?
555
N
Y
Return to Shipper
565
Decrypt With Private Key
540
Hash
541
Extract Identity
545
Hash
=?
550
Y
N
Forward to Next Destination
570
Authorized Receiver ?
585
Yes
No
Deliver Package
590
Return to Sender
595

Figure 11

INTERNATIONAL SEARCH REPORT

Intern. nal Application No
PCT/US 00/27261

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C G06K G06F A61B G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 99 52422 A (BEECHAM JAMES E) 21 October 1999 (1999-10-21) abstract; figures page 6, line 27 -page 9, line 35 page 11, line 31 -page 14, line 32 page 28, line 28 -page 31, line 31	1-33
Y	US 5 153 842 A (CHEN ROBERT ET AL) 6 October 1992 (1992-10-06) abstract; claims; figures column 8, line 8 -column 11, line 11	1-33
A	US 5 038 283 A (CAVENEY JACK E) 6 August 1991 (1991-08-06) abstract; claims; figures	1,12,14, 15,17, 18,22, 28,29,31

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 January 2001	29/01/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax (+31–70) 340–3016	Meyl, D

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/US 00/27261

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 863 491 A (BRITISH TELECOMM) 9 September 1998 (1998-09-09)	

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr. nal Application No
PCT/US 00/27261

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9952422 A	21-10-1999	AU 3641899 A	01-11-1999
US 5153842 A	06-10-1992	NONE	
US 5038283 A	06-08-1991	CA 2013716 A	13-10-1990
		DE 4011994 A	18-10-1990
		FR 2645992 A	19-10-1990
		GB 2234229 A,B	30-01-1991
		IT 1251520 B	16-05-1995
		JP 3003071 A	09-01-1991
EP 0863491 A	09-09-1998	WO 9839740 A	11-09-1998
		AU 6628998 A	22-09-1998
		EP 0966729 A	29-12-1999